ELSEVIER Linear Algebra and its Applications 331 (2001) 31–41

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

The product of two quadratic matrices

Florian Bünger, Frieder Knüppel*, Klaus Nielsen

Mathematisches Seminar, Christian-Albrechts-Universität zu Kiel, Ludewig-Meyn-Strasse 4, D-24098 Kiel, Germany

Received 7 August 2000; accepted 11 January 2001

Submitted by R.A. Brualdi

Abstract

Let $p = (x - \beta)(x - \beta^{-1}) \in K[x]$ where $\beta^2 \neq \beta^{-2}$ and let V be a finite-dimensional vector space over the field K. A linear mapping $M : V \to V$ is called quadratic if $p(M) = 0$. We characterize products of two quadratic linear mappings. © 2001 Elsevier Science Inc. All rights reserved.

Keywords: Matrices of quadratic type; Products of matrices; Factorization of matrices

1. Introduction and main result

Let K be a commutative field, $n \in \mathbb{N}$ and $p \in K[x]$ a polynomial of degree 2.

We write GL_n for the group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices with entries in K.

Definition 1.1 (*quadratic matrix*). A matrix $M \in K^{n\times n}$ is called quadratic (for the polynomial p) if $p(M) = 0$; that is, the minimum polynomial of the matrix M divides p. Call a matrix A 2-quadratic (for p) if it is the product of two quadratic matrices (for p).

If M is similar to N and M is 2-quadratic, then N is also 2-quadratic.

If $p = x^2 - 1$, then M is quadratic if and only if M is an involution. In this case it is well known that a matrix A is 2-quadratic if and only if A is similar to its inverse. These matrices can easily be described in terms of their elementary divisors; cf. [2].

Let I denote an identity matrix (of suitable dimension).

* Corresponding author.

PII: S 0 0 2 4 - 3 7 9 5 (0 1) 0 0 2 7 7 - 4

Let $p = (x-\beta)(x-\beta^{-1}) \in K[x]$, where $\beta^2 \neq \beta^{-2}$. If $K = \mathbb{C}$, then Wang [4] gave a description of 2-quadratic matrices. The present paper is a generalization to arbitrary fields.

Theorem 1.2. *Let $p = (x-\beta)(x-\beta^{-1}) \in K[x]$, where $\beta^2 \neq \beta^{-2}$. Let $n \in \mathbb{N}$ and $M \in K^{n\times n}$. Then M is 2-quadratic (for p) if and only if up to similarity M has the form $M = X \oplus Y \oplus Z_+ \oplus Z_-$, where*

(i) *X is similar to X^{-1}, and* $\operatorname{char} K = 2$ *or X does not have elementary divisors $(x+1)^{2t+1}$ for $t \in \mathbb{N}_0$.*
(ii) *$Y = (\beta^2 I + ST) \oplus (\beta^2 I + TS)^{-1}$, where $S \in K^{r\times s}$, $T \in K^{s\times r}$ and ST as well as TS are nilpotent.*
(iii) *$Z_+ = \beta^2 I$ and $Z_- = \beta^{-2} I$.*

2. Preliminaries

We will frequently use a theorem due to Roth. For a proof we refer to [1, Satz 3.7].

Theorem 2.1 (Roth). *Let $r, s \in \mathbb{N}$, $A \in \mathrm{GL}_r$, $B \in \mathrm{GL}_s$ and $C \in K^{r\times s}$. Then the matrix equation $AX - XB = C$ has a solution $X \in K^{r\times s}$ if and only if the matrices*

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} A & C \\ 0 & B \end{bmatrix}$$

are similar.

Corollary 2.2. *Let $r, s \in \mathbb{N}$, $A \in \mathrm{GL}_r(K)$ and $B \in \mathrm{GL}_s(K)$. If* $\operatorname{char} A$ *is prime to* $\operatorname{char} B$, *then the linear mapping*

$$\tau_{A,B} : K^{r\times s} \to K^{r\times s}, \quad X \mapsto AX - XB$$

is an isomorphism.

Indeed, the mapping is surjective by the above theorem.

2.1. Basic assumption and definition

In the sequel we consider a quadratic polynomial $p = x^2 + \nu x + \epsilon$, where $\nu \in K$ and $\epsilon \in \{1, -1\}$.

Let $q := x^2 + (2\epsilon - \nu^2)x + 1$ (observe: if γ is a zero of p, then γ^2 is a zero of q).

We call $M \in K^{n\times n}$ quadratic if $p(M) = 0$. Further, M is called 2-quadratic if M is a product of two quadratic matrices.

Remark 2.3. Let $X \in \mathrm{GL}_r(K)$ and $Y \in \mathrm{GL}_s(K)$, where $r, s \in \mathbb{N}$ and $A := X \oplus Y$. Let

$$B := \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}, \quad C := \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

be quadratic matrices such that $A = BC$ (where $B_{11}, C_{11} \in K^{r\times r}$; $B_{12}, C_{12} \in K^{r\times s}$; $B_{21}, C_{21} \in K^{s\times r}$; $B_{22}, C_{22} \in K^{s\times s}$).

Since

$$B^2 + \nu B + \epsilon I = p(B) = 0 = p(C) = C^2 + \nu C + \epsilon I,$$

we have $B^2 = -\nu B - \epsilon I$ and $C^2 = -\nu C - \epsilon I$. Therefore,

$$\begin{bmatrix} B_{11}X & B_{12}Y \\ B_{21}X & B_{22}Y \end{bmatrix} = BA = B^2C = -\nu A - \epsilon C$$

$$= -\begin{bmatrix} \nu X + \epsilon C_{11} & \epsilon C_{12} \\ \epsilon C_{21} & \nu Y + \epsilon C_{22} \end{bmatrix}$$

and

$$\begin{bmatrix} XC_{11} & XC_{12} \\ YC_{21} & YC_{22} \end{bmatrix} = AC = BC^2 = -\nu A - \epsilon B$$

$$= -\begin{bmatrix} \nu X + \epsilon B_{11} & \epsilon B_{12} \\ \epsilon B_{21} & \nu Y + \epsilon B_{22} \end{bmatrix}.$$

Corollary 2.4. *Under the assumptions of the previous remark we have*

(a) (1) $B_{11}X = -\nu X - \epsilon C_{11}$, (2) $X(C_{11} + \nu I) = -\epsilon B_{11}$.

(b) $X^{-1}B_{11} - B_{11}X = \nu(X - \epsilon I)$.
If additionally $\epsilon I + X \in \mathrm{GL}_r$ *and* $\operatorname{char} X$ *is prime to* $\operatorname{char}(X^{-1})$, *then* $B_{11} = -\nu X(\epsilon I + X)^{-1}$.

(c) *Suppose that* $\epsilon I + X \in \mathrm{GL}_r$ *and that* $\operatorname{char} X$ *is prime to* $\operatorname{char}(X^{-1})$ *and the analogue holds true for Y. Then*

$$B_{12}B_{21} = -\epsilon(\epsilon I + X)^{-2}q(X) \quad \text{and} \quad B_{21}B_{12} = -\epsilon(\epsilon I + Y)^{-2}q(Y).$$

Proof. The matrix identities in Remark 2.3 entrain (1) and (2) of (a). Statement (b) follows from (a).

For the second claim we observe that the matrix $Z := -\nu X(\epsilon I + X)^{-1}$ satisfies $X^{-1}Z - ZX = \nu(X - \epsilon I)$. Hence $Z = B_{11}$ by Corollary 2.2 and the first statement in (b).

(c) As $p(B) = 0$ we have $B_{12}B_{21} = -p(B_{11})$. Taking B_{11} from (b) yields the assertion. □

Corollary 2.5. *Consider the assumptions of the previous corollary, part* (c). *Suppose that* $p = (x-\beta)(x-\epsilon\beta^{-1})$, *hence* $q = (x-\beta^2)(x-\beta^{-2})$. *Further, suppose that* $X-\beta^{-2}I$ *and* $Y-\beta^2 I$ *are invertible. Let* $S := -\epsilon(\epsilon I+X)^2(X-\beta^{-2})^{-1}B_{12}$ *and* $T := B_{21}$.

Then $X = ST+\beta^2 I$ *and* $Y^{-1} = TS+\beta^2 I$.

Proof. The identity $X = ST+\beta^2 I$ follows immediately from part (c) of Corollary 2.5. In order to calculate $TS = Y^{-1}-\beta^2 I$ we use (+) $B_{21}X = Y^{-1}B_{21}$ (which is obvious from the matrix identities in Remark 2.3) and (++) $B_{21}(X-\beta^{-2})^{-1} = (Y^{-1}-\beta^{-2})^{-1}B_{21}$ (this follows from (+)) and apply once more part (c) of Corollary 2.5. □

Lemma 2.6. *Let* $p = (x-\beta)(x-\beta^{-1})$ *and* $\beta^2 \neq \beta^{-2}$. *Let* $s, t \in \mathbb{N}$ *and* $S \in K^{r\times s}$ *and* $T \in K^{s\times r}$ *such that ST and TS are nilpotent matrices.*

Put $X := \beta^2 I+ST$ *and* $Y' := \beta^2 I+TS$ *and* $A := X\oplus Y$, *where* $Y := Y'^{-1}$ (*observe that* $X \in \mathrm{GL}_r$ *and* $Y' \in \mathrm{GL}_s$).

Then A is 2*-quadratic.*

Proof. Let $B_{11} := \beta I+\beta^{-1}ST$, $B_{12} := -\beta S-\beta^{-1}STS+\beta^{-1}S$, $B_{21} := \beta^{-1}T$, $B_{22} := \beta^{-1}I-\beta^{-1}TS$, $C_{11} := \beta I$, $C_{12} := \beta^{-1}S-\beta^{-2}(\beta I+\beta^{-1}ST)^{-1}S$, $C_{21} := 0$, $C_{22} := \beta^{-1}I$. Let B and C be the matrices given by these submatrices. Then B and C are quadratic and

$$BC = \begin{bmatrix} X & 0 \\ T & Y \end{bmatrix}.$$

We now use that ST and TS are nilpotent mappings. This yields that $\mathrm{char}X = (x-\beta^2)^r$ and $\mathrm{char}Y = (x-\beta^{-2})^s$. As $\beta^2 \neq \beta^{-2}$ the two polynomials are prime. Hence BC is similar to A. □

Corollary 2.7. *Let* $p = (x-\beta)(x-\beta^{-1})$ *and* $\beta^2 \neq \beta^{-2}$. *Let* $n \in \mathbb{N}$ *and* $A \in \mathrm{GL}_n$ *such that* $\mathrm{char}\,A = (x-\beta^2)^r(x-\beta^{-2})^s$, *where* $r, s \in \mathbb{N}$. *Then A is* 2*-quadratic if and only if A has* (*up to similarity*) *the form* $A = (\beta^2 I+ST)\oplus(\beta^2 I+TS)^{-1}$, *where* $S \in K^{r\times s}$, $T \in K^{s\times r}$ *and ST as well as TS are nilpotent matrices.*

Proof. Suppose that $\mathrm{char}\,A = (x-\beta^2)^r(x-\beta^{-2})^s$, where $r, s \in \mathbb{N}$. Since the two factors are prime we have $A = X\oplus Y$, where $\mathrm{char}\,X = (x-\beta^2)^r$ and $\mathrm{char}\,Y = (x-\beta^{-2})^s$. If A is 2-quadratic, then Corollary 2.5 supplies a pair of matrices S, T such that A has the required form. Lemma 2.6 provides the converse assertion. □

Lemma 2.6 and Corollary 2.5 can be obtained from [3].

Lemma 2.8. *Let* $X \in \mathrm{GL}_r(K)$ *and* $Y \in \mathrm{GL}_s(K)$, $r+s = n$, *and* $\mathrm{char}(X^{-1})$ *prime to* $\mathrm{char}(Y)$. *If* $A := X\oplus Y$ *is* 2*-quadratic, then X and Y are also* 2*-quadratic.*

Proof. From the identity $A = BC$ in Remark 2.3 we obtain $B_{12}Y = X^{-1}B_{12}$ and $YC_{21} = C_{21}X^{-1}$. As $\mathrm{char}(X^{-1})$ is prime to $\mathrm{char}(Y)$ Corollary 2.2 implies that $B_{12} = 0$ and $C_{21} = 0$; hence also C_{12} and $B_{21} = 0$. We conclude that each of the matrices $B_{11}, B_{22}, C_{11}, C_{22}$ is quadratic and $X = B_{11}C_{11}$ and $Y = B_{22}C_{22}$. □

Remark 2.9. *Let $M = AB$, where A and B are quadratic. Then*
(i) $A^{-1} = -\epsilon(A + \nu I)$.
(ii) $M^{-1} = BA + \nu(A + B) + \nu^2 I$.
(iii) $(A - B)M = M^{-1}(A - B)$.
(iv) $A(M + M^{-1}) = (M + M^{-1})A$ *and* $B(M + M^{-1}) = (M + M^{-1})B$.

Proof. As $A^2 + \nu A + \epsilon I_n = 0$ statement (i) holds true. Now (i) and $\epsilon^2 = 1$ yield

$$M^{-1} = B^{-1}A^{-1} = (B + \nu I)(A + \nu I) = BA + \nu(A + B) + \nu^2 I.$$

Also (iii) and (iv) are obtained from simple calculations. □

Corollary 2.10. *Let $M = AB$, where A, B are quadratic matrices and the characteristic polynomials of M and M^{-1} are prime. Then $A = B$. In particular $q(M) = 0$.*

Proof. Statement (iii) of Remark 2.9 and Corollary 2.2 imply $A - B = 0$. □

Corollary 2.11. *Suppose that $p = (x - \beta)(x - \epsilon\beta^{-1})$, where $\beta^2 \neq \beta^{-2}$. Let $M \in \mathrm{GL}_n$ be 2-quadratic and $(M - \beta^2 I)^n = 0$ or $(M - \beta^{-2}I)^n = 0$. Then $M = \beta^2 I$, respectively $M = \beta^{-2}I$.*

Proof. The minimum polynomial of M divides $q = (x - \beta^2)(x - \beta^{-2})$ (by Corollary 2.10) and $(x - \beta^2 I)^n$, respectively $(x - \beta^{-2}I)^n$. □

Corollary 2.12. *Suppose that M is 2-quadratic and* char M *is prime to q. Then M is similar to M^{-1}.*

Proof. Let $Q := A - B$, where $M = AB$ and A, B are quadratic. From Remark 2.9 (ii) it follows that

$$\begin{aligned} Q^2 &= A^2 + B^2 - AB - BA \\ &= -\nu(A + B) - 2\epsilon I - M - M^{-1} + \nu(A + B) + \nu^2 I \\ &= -M - M^{-1} - (2\epsilon - \nu^2)I. \end{aligned}$$

Hence $-Q^2 M = q(M)$. As $\mathrm{char}\, M$ is prime to q we have $q(M) \in \mathrm{GL}_n$. Thus Q is invertible and Remark 2.9(iii) yields that $QMQ^{-1} = M^{-1}$. □

2.2. Assumption

For the rest of this paper we assume that $p = (x-\beta)(x-\beta^{-1})$, where $\beta^2 \neq \beta^{-2}$.

Lemma 2.13. *If $M \in \mathrm{GL}_n$ has an elementary divisor $(x+1)^{2t+1}$, where $t \in \mathbb{N}_0$ and* char $K \neq 2$, *then M is not 2-quadratic.*

Proof. Let $M = AB$, where A and B are quadratic matrices. In Remark 2.9(iv) we noticed that A commutes with $M + M^{-1}$, hence also with $(M+I)^2M^{-1} = M + M^{-1} + 2I$. This implies that $\mathrm{kernel}(M+I)^{2m}$ is invariant under M, A and B for each $m \in \mathbb{N}_0$. Now we have an elementary divisor $(x+1)^{2t+1}$ for M. By the above observation A, B and M induce linear mappings A', B', M' on the space

$$W := \mathrm{kernel}(M+I)^{2t+2}/\mathrm{kernel}(M+I)^{2t}.$$

Clearly, A' and B' are quadratic and $M' = A'B'$. Further, M' has an elementary divisor $x+1$, and the minimum polynomial of M' divides $(x+1)^2$. This yields $\dim(\mathrm{kernel}(M'+I)) > \frac{1}{2}\dim W$. As $W = \mathrm{kernel}(A'-\beta I) \oplus \mathrm{kernel}(A'-\beta^{-1}I)$ we have $\mathrm{kernel}(M'+I) \cap \mathrm{kernel}(A'-\beta I) \neq 0$ or $\mathrm{kernel}(M'+I) \cap \mathrm{kernel}(A'-\beta^{-1}I) \neq 0$. Hence $-\beta^{-1}$ or $-\beta$ is an eigenvalue for B', and hence an element of $\{\beta, \beta^{-1}\}$. This is a contradiction. □

Lemma 2.14. *Let $M \in \mathrm{GL}_{2m}$ such that M is similar to M^{-1}, and* char $K = 2$ *or $(x+1)^{2t+1}$ is not an elementary divisor of M ($t \in \mathbb{N}_0$).*

Then M is 2-quadratic.

Proof. In Appendix A we will prove that (up to similarity)

$$M = \begin{bmatrix} I & B \\ A & I + AB \end{bmatrix}$$

for some matrices $A, B \in K^{m\times m}$. Let

$$S := \begin{bmatrix} P & 0 \\ AP & Q \end{bmatrix} \quad \text{and} \quad T := \begin{bmatrix} P^{-1} & P^{-1}B \\ 0 & Q^{-1} \end{bmatrix},$$

where $P, Q \in \mathrm{GL}_m$ are arbitrary invertible matrices. Then $M = ST$. Now take $P := \beta I$ and $Q := \beta^{-1}I$. Then S and T are quadratic. □

Lemma 2.15. *Let $M \in \mathrm{GL}_n$ and* char $M = (x-1)^n$, *i.e. M is unipotent. Then M is 2-quadratic.*

Proof. We may assume that M is a cyclic mapping. Then M is similar to its inverse. If $\dim V$ is even, then the previous lemma includes the assertion. Assume that n is odd. Let

$$D := \begin{bmatrix} \beta & 1 \\ 0 & \beta^{-1} \end{bmatrix}, \quad B := \operatorname{diag}(D, \ldots, D, \beta), \quad C := \operatorname{diag}(\beta^{-1}, D, \ldots, D)$$

(D occurs in each matrix $\frac{1}{2}(n-1)$ times). Then B and C are quadratic matrices and BC is an upper diagonal matrix where all diagonal entries are 1 and the entries in the upper diagonal are $\beta, \beta^{-1}, \beta, \beta^{-1}, \ldots$ Hence $\operatorname{char}(BC) = (x-1)^n$ and BC is cyclic. This implies that BC is similar to M. □

Corollary 2.16. *Let $M \in \mathrm{GL}_n$ such that M is similar to M^{-1}, and* char $K = 2$ *or $(x+1)^{2t+1}$ is not an elementary divisor of M for any $t \in \mathbb{N}_0$.*

Then M is 2-quadratic.

Proof. We write $M = M_1 \oplus M_2$, where char M_1 is prime to $x-1$ and char $M_2 = (x-1)^m$. It follows that M_1 has even dimension (see Appendix A) and it is similar to its inverse. Hence M_1 is 2-quadratic by Lemma 2.14. Further, M_2 is 2-quadratic by Lemma 2.15. □

Proof of Theorem 1.2. ($\Rightarrow$) Let M be 2-quadratic. Then M does not have elementary divisors $(x+1)^{2t+1}$ for $t \in \mathbb{N}_0$ or char $K = 2$; cf. Lemma 2.13. We write $M = X \oplus Y$ where char X is prime to $q = (x-\beta^2)(x-\beta^{-2})$ and $\operatorname{char}(Y) = (x-\beta^2)^r(x-\beta^{-2})^s$ for appropriate $r, s \in \mathbb{N}_0$. Then X and Y are 2-quadratic by Lemma 2.8. Further, X is similar to X^{-1}; cf. Corollary 2.12. As to Y, three distinct cases can occur (provided that $Y \neq 0$): $r = 0 \neq s$; $r \neq 0 = s$; $r \neq 0 \neq s$. In the first two cases Corollary 2.11 implies that $Y = \beta^{-2}I$, respectively $Y = \beta^2 I$. In the last case Corollary 2.7 (where Y_1 corresponds to X and Y_2 to Y) provides matrices S, T such that $Y = Y_1 \oplus Y_2$ and $Y_1 = \beta^2 I + ST$ and $Y_2^{-1} = \beta^2 I + TS$ and ST, TS are nilpotent.

We proved that M has the desired form.

($\Leftarrow$) Suppose that $M = X \oplus Y \oplus Z_- \oplus Z_+$, where

(i) X is similar to X^{-1}, and X does not have elementary divisors $(x+1)^{2t+1}$ for $t \in \mathbb{N}_0$ or char $K = 2$;

(ii) $Y = (\beta^2 I + ST) \oplus (\beta^2 I + TS)^{-1}$, where $S \in K^{r\times s}$, $T \in K^{s\times r}$ and ST as well as TS are nilpotent;

(iii) $Z_+ = \beta^2 I$ and $Z_- = \beta^{-2} I$.

Then X is 2-quadratic by Corollary 2.16; Y is 2-quadratic by Corollary 2.7; Z_+ is obviously 2-quadratic as βI is quadratic and Z_- is also 2-quadratic. Hence M is 2-quadratic. □

Appendix A

The following crucial proposition was used in the proof to our theorem.

Proposition A.1. *Let* $\dim V = 2m$ *even and $M \in \mathrm{GL}_{2m}$ similar to its inverse M^{-1}. If* char $K = 2$ *or M does not have an elementary divisor $(x+1)^{2t+1}$ ($t \in \mathbb{N}_0$), then M is similar to a matrix of the form*

$$M = \begin{bmatrix} I & B \\ A & I + AB \end{bmatrix},$$

where $A, B, I \in K^{m\times m}$.

In the sequel we provide a proof.

It is well known that a linear bijection $\pi : V \to V$ (where $V \neq 0$ is a finite-dimensional vector space over a field K) is a product of two involutions if and only if π is similar to its inverse; see e.g. [2].

We need some information on the possible choice of the two involutions in order to prove Proposition A.2.

The subspace $B(\pi) := V(\pi - 1)$ is called the path of the linear mapping $\pi : V \to V$; $F(\pi) := \text{kernel}(\pi - 1)$ the fixed space of π and $\mathrm{N}(\pi) := \text{kernel}(\pi + 1)$ the negative space of π.

For linear mappings $\pi, \varphi : V \to V$ one has $B(\varphi\pi) \subseteq B(\varphi) + B(\pi)$ ('path-lemma').

Let $\sigma : V \to V$ be a linear bijection. Then σ is an involution if and only if $B(\sigma) \subseteq \mathrm{N}(\sigma)$. When $\operatorname{char} K \neq 2$ then $\subseteq$ can be replaced by $=$, and one has $V = F(\sigma) \oplus \mathrm{N}(\sigma)$.

Observe that $\operatorname{char} K = 2$ entails $\mathrm{N}(\pi) = F(\pi)$ for each linear mapping π.

Proposition A.2. *Assume that* $\dim V = 2m$ *is even. Let* $\pi : V \to V$ *be a linear bijection that is similar to its inverse.*

(a) *Let* $\operatorname{char} K \neq 2$ *and suppose that* π *does not have elementary divisors* $(x + 1)^{2t+1}$, *where* $t \in \mathbb{N}_0$. *Then* $\pi = \rho\sigma$ *for involutions* ρ, σ *such that* $V = B(\rho) \oplus F(\sigma)$ *and* $\dim B(\sigma) = m = \dim F(\rho)$.

(b) *Let* $\operatorname{char} K = 2$. *Then* $\pi = \rho\sigma$ *for involutions* ρ, σ *such that* $V = U \oplus W$ *for appropriate subspaces* U, W *with* $B(\rho) \subseteq U \subseteq F(\rho)$ *and* $B(\sigma) \subseteq W \subseteq F(\sigma)$ *and* $\dim U = m = \dim W$.

Indeed Proposition A.2 entrains Proposition A.1 as we shall see now. Select ρ, σ as in Proposition A.2. If $\operatorname{char} K = 2$ let U, W as in (b) of that proposition, else $U := B(\rho)$ and $W := F(\sigma)$. Putting together a basis for U and a basis for W we obtain a basis for V. The matrix-representations of ρ and σ in this basis are

$$\rho = \begin{bmatrix} -I & 0 \\ A & I \end{bmatrix} \quad \text{and} \quad \sigma = \begin{bmatrix} -I & B \\ 0 & I \end{bmatrix}.$$

Hence π has a matrix-representation as stated in Proposition A.1.

We will provide a proof to Proposition A.2 in several steps.

1. For a polynomial $f(x)$ of degree n with $f(0) \neq 0$ let $f^*(x) := f(0)^{-1}x^n f(x^{-1})$ denote its 'reciprocal' polynomial. If $f = f_1 \cdots f_k$, then $f^* = f_1^* \cdots f_k^*$. Call f symmetric if $f = f^*$. For $\pi \in GL$ it is easy to see that $\operatorname{char} \pi^{-1} = (\operatorname{char} \pi)^*$, and $\operatorname{mip} \pi^{-1} = (\operatorname{mip} \pi)^*$ for the characteristic and the minimum polynomials. Hence, if

π is similar to π^{-1}, then the characteristic polynomial of π is symmetric and the minimal polynomial of π is symmetric.

2. Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a monic symmetric polynomial. Then $a_i = a_{n-i}$ for $i \in \{0, \ldots, n\}$ or $a_i = -a_{n-i}$ for $i \in \{0, \ldots, n\}$. Hence -1 or 1 is a zero of f whenever n is odd. Therefore, the only monic irreducible symmetric polynomials of odd degree are $x - 1$ and $x + 1$.

3. Let π be a linear bijection of a vectorspace $V \to V$ (over a commutative field K) such that π is similar to its inverse. Then we have a decomposition $V = V_1 \oplus \cdots \oplus V_r \oplus V_1' \oplus V_1'' \oplus \cdots \oplus V_s' \oplus V_s''$ such that

(i) each V_i, V_i', V_i'' is an irreducible π-module;
(ii) the minimal polynomial of the restriction π_{V_i} has the form $p_i^{m_i}$ where p_i is a symmetric monic irreducible polynomial;
(iii) the minimal polynomial of the restriction $\pi_{V_i'}$ has the form $q_i^{k_i}$, where q_i is a monic irreducible polynomial that is prime to its reciprocal q_i^*, and $(q_i^*)^{k_i}$ is the mimimal polynomial of the restriction $\pi_{V_i''}$.

In particular, each V_i is a cyclic π-module such that the restriction π_{V_i} has a symmetric minimal polynomial $p_i^{m_i}$, and also each $V_i' \oplus V_i''$ is a cyclic π-module such that the restriction of π has the symmetric minimal polynomial $(q_i q_i^*)^{k_i}$.

Using the above facts one deduces that each of the above-mentioned restrictions of π is a product of two involutions, and hence π is a product of two involutions. See e.g. [2].

Clearly, each module $V_i' \oplus V_i''$ has even dimension.

Further, by our discussion on symmetric polynomials, each V_i has even dimension except when $p_i^{m_i} = (x-1)^{m_i}$ or $p_i^{m_i} = (x+1)^{m_i}$.

4. In the sequel let $\pi = \rho\sigma$, where $\rho, \sigma : V \to V$ are linear involutions and $n := \dim V$.

4.1 Remark. $\pi = \sigma\rho^\sigma$, so σ can be put to the first place.

We need additional informations compiled in the following lemmas.

5.1 Lemma. *Let $n = \dim V = 2m$ even, π a cyclic mapping and $F(\pi) = 0$ or $N(\pi) = 0$. Then $\dim B(\rho) = m = \dim B(\sigma)$, and $V = F(\rho) \oplus B(\sigma)$ or $V = F(\sigma) \oplus B(\rho)$ (when $\operatorname{char} K = 2$ then both are true).*

Proof. The assumptions yield
(0) $\dim B(\pi) \geqslant n - 1$,
(1) $B(\pi) \subseteq B(\rho) + B(\sigma) \subseteq V$ ('path-lemma')
(2) $\dim((B(\rho) \cap B(\sigma)) + (F(\rho) \cap F(\sigma))) \leqslant \dim F(\pi) \leqslant 1$,
(3) $\dim((F(\sigma) \cap B(\rho)) + (F(\rho) \cap B(\sigma))) \leqslant \dim N(\pi) \leqslant 1$.

Hence
(4) $n - 1 \leqslant \dim B(\rho) + \dim B(\sigma) \leqslant n + 1$ (due to (0), (1) and (2)), and
(5) $|\dim B(\rho) - \dim B(\sigma)| \leqslant 1$ (due to (2) and (3)).

We may assume that $\dim B(\rho) \geqslant \dim B(\sigma)$. If $\dim B(\rho) = m$ and $\dim B(\sigma) = m - 1$, then (2) and (3) yield $F(\pi) \neq 0 \neq N(\pi)$, a contradiction. Similarly, when $\dim B(\rho) = m + 1$ and $\dim B(\sigma) = m$. Hence $\dim B(\rho) = m = \dim B(\sigma)$ is the only possibility. The remaining assertion follows in the case of $\operatorname{char} K \neq 2$ from (3) and $V = B(\rho) \oplus F(\rho)$. If $\operatorname{char} K = 2$, then $F(\pi) = N(\pi) = 0$ by assumption and the assertion is obvious. □

Similar arguments yield the following lemmas. We omit the proofs.

5.2 Lemma. *Let* $\operatorname{char} K \neq 2$ *and* π *cyclic with characteristic polynomial* $(x-1)^{2t+1}$. *Then*

$$\dim F(\rho) = \dim F(\sigma) = t \quad \textit{and} \quad \dim B(\rho) = \dim B(\sigma) = t + 1$$

or

$$\dim F(\rho) = \dim F(\sigma) = t + 1 \quad \textit{and} \quad \dim B(\rho) = \dim B(\sigma) = t.$$

Further, $V = F(\rho) \oplus B(\sigma) = F(\sigma) \oplus B(\rho)$.

5.3 Lemma. *Let* $\operatorname{char} K = 2$ *and* π *cyclic with characteristic polynomial* $(x-1)^{2t+1}$. *Then* $\dim B(\rho) = t = \dim B(\sigma)$, $B(\pi) = B(\rho) \oplus B(\sigma)$, $F(\pi) = F(\rho) \cap F(\sigma)$ *and* $V = F(\rho) \oplus B(\sigma)$ *or* $V = F(\sigma) \oplus B(\rho)$.

5.4 Lemma. *Let* $\operatorname{char} K = 2$ *and* π *cyclic with characteristic polynomial* $(x-1)^{2t}$. *Then* $B(\rho) \cap F(\pi) = 0$ *or* $B(\sigma) \cap F(\pi) = 0$. *In the second case,* $F(\rho) = B(\rho)$ *is* t*-dimensional, and* $\dim F(\sigma)/B(\sigma) = 2$ *and* $B(\pi) = B(\rho) \oplus B(\sigma)$ *and* $V = F(\rho) \oplus W$ *for a subspace* W *such that* $B(\sigma) \subseteq W \subseteq F(\sigma)$.

5.5 Proof of Proposition A.2. Consider a decomposition of V into π-modules as in 3.

If a π-module satisfies the requirements of Lemma 5.1 (i.e. its dimension is even and $F(\pi) = 0$ or $N(\pi) = 0$), then the assertion of Proposition A.2 is true for this π-module (by 5.1 and 5.0).

Hence we can delete π-modules that fit into Lemma 5.1.

We pursue the cases $\operatorname{char} K \neq 2$, respectively $\operatorname{char} K = 2$ separately.

If $\operatorname{char} K \neq 2$, the only remaining π-modules (i.e. those not covered by Lemma 5.1) are the ones considered in Lemma 5.2, and their number is even. So it suffices to consider a direct sum of two modules of that type. Using Lemma 5.2 and Remark 5.0 we see that the assertion of Proposition A.2 is true for such a pair.

Finally, let $\operatorname{char} K = 2$. The only remaining π-modules are associated with characteristic polynomials $(x-1)^s$.

If s is even, then Lemma 5.4 and Remark 5.0 prove the assertion of Proposition A.2 for such a π-module.

Hence we need only consider the case that V is the direct sum of two π-modules associated with minimal polynomials $(x-1)^{2t_1+1}$, respectively $(x-1)^{2t_2+1}$. Using 5.0 and 5.3 we obtain the assertion.

The proof to Proposition A.2 is finished. □

References

[1] F. Bünger, I Produkte von Konjugiertenklassen in den Gruppen GL(V) und SL(V) II Der Satz von Roth über kommutativen Ringen, Diplomarbeit Kiel, 1994.
[2] D.Ž. Doković, Product of two involutions, Arch. Math. 18 (1967) 582–584.
[3] H. Flanders, Elementary divisors of AB and BA, Proc. Am. Math. Soc. 2 (1951) 871–874.
[4] J.-H. Wang, Products of invertible operators of quadratic type, Linear Algebra Appl. 245 (1996) 1–26.